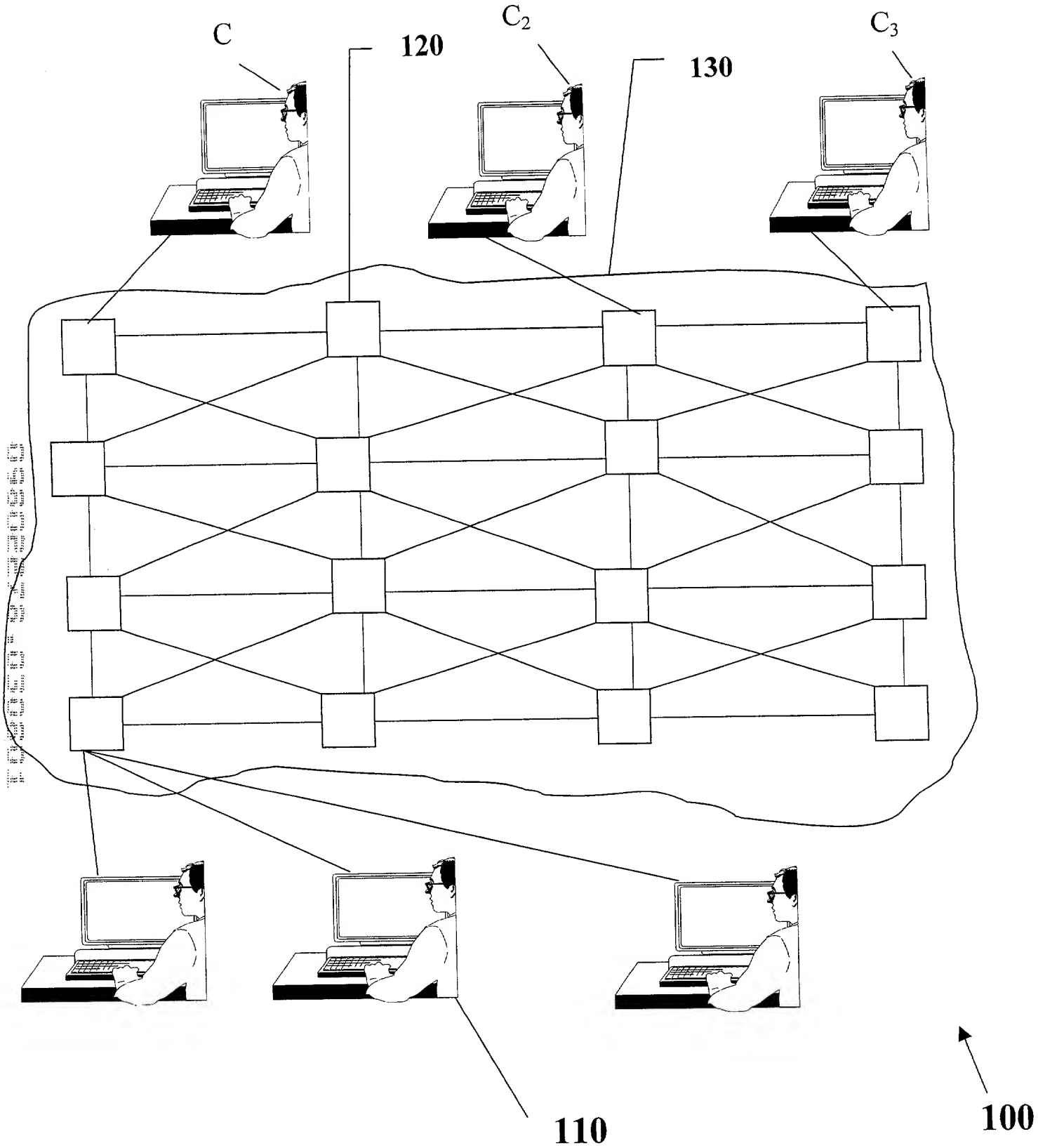

FIGURE 1

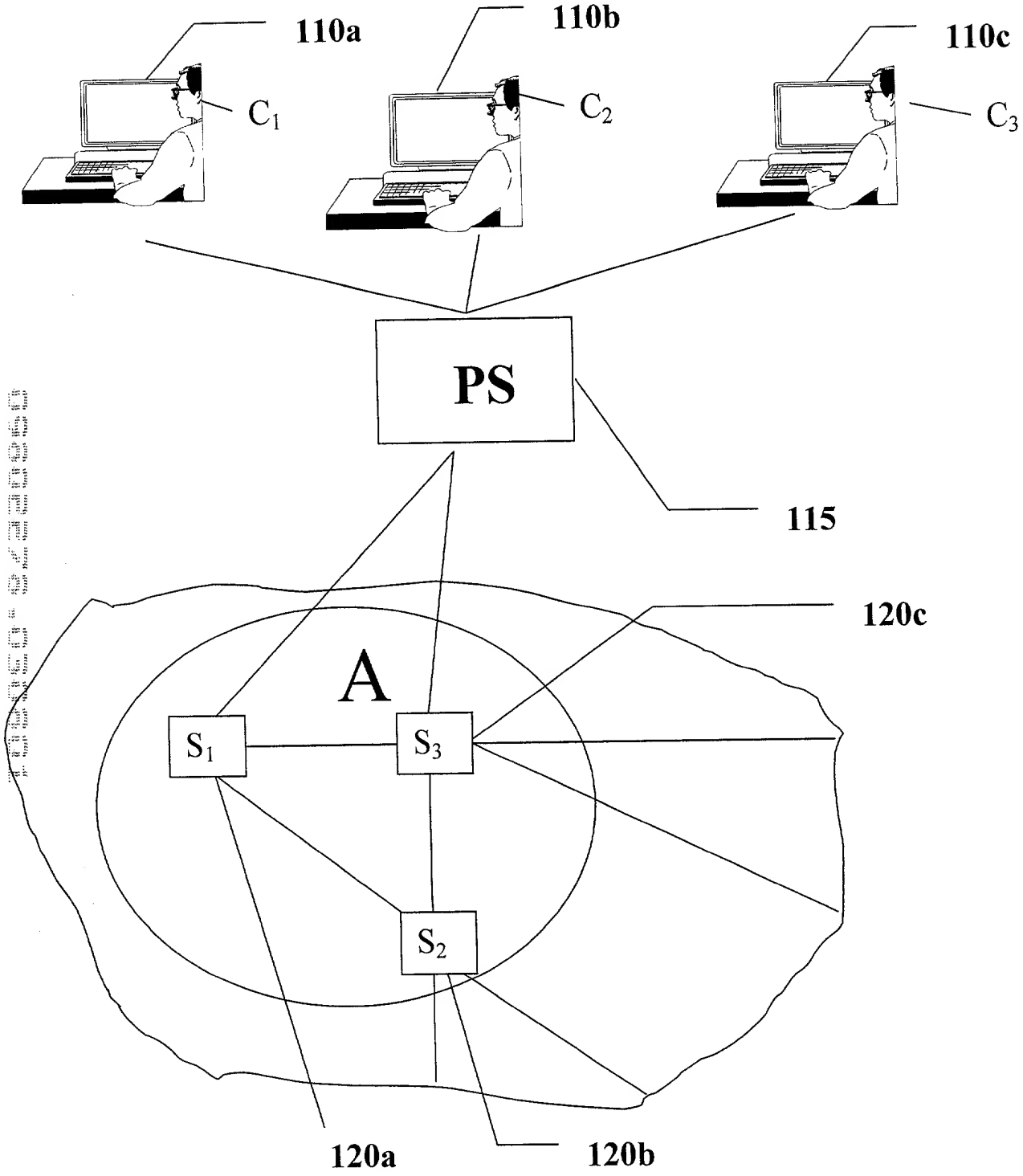

FIGURE 2

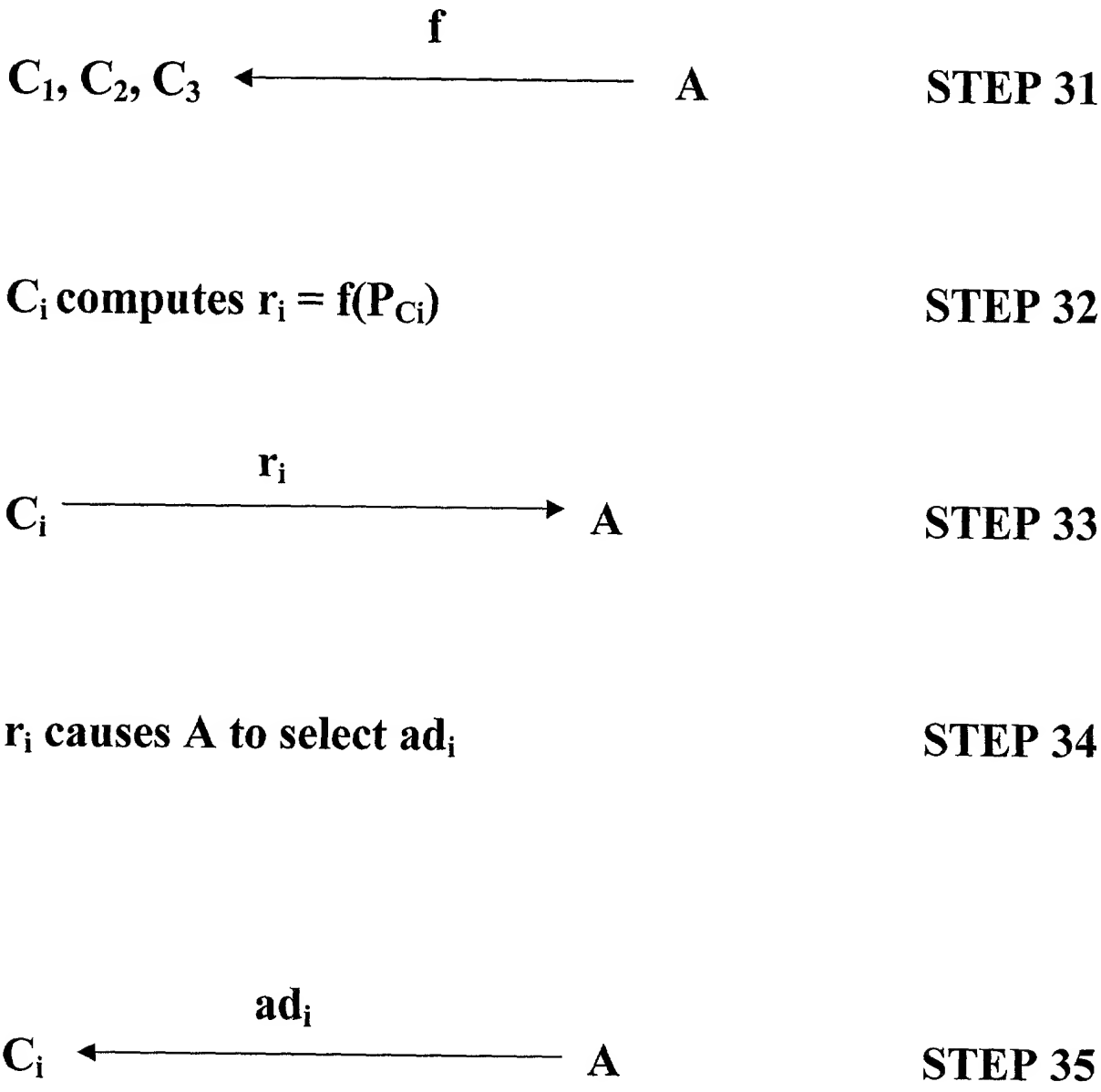
f
C1, C2, C3
A
STEP 31
Ci computes ri = f(PCi)
STEP 32
ri
Ci
A
STEP 33
ri causes A to select adi
STEP 34
adi
Ci
A
STEP 35

FIGURE 3

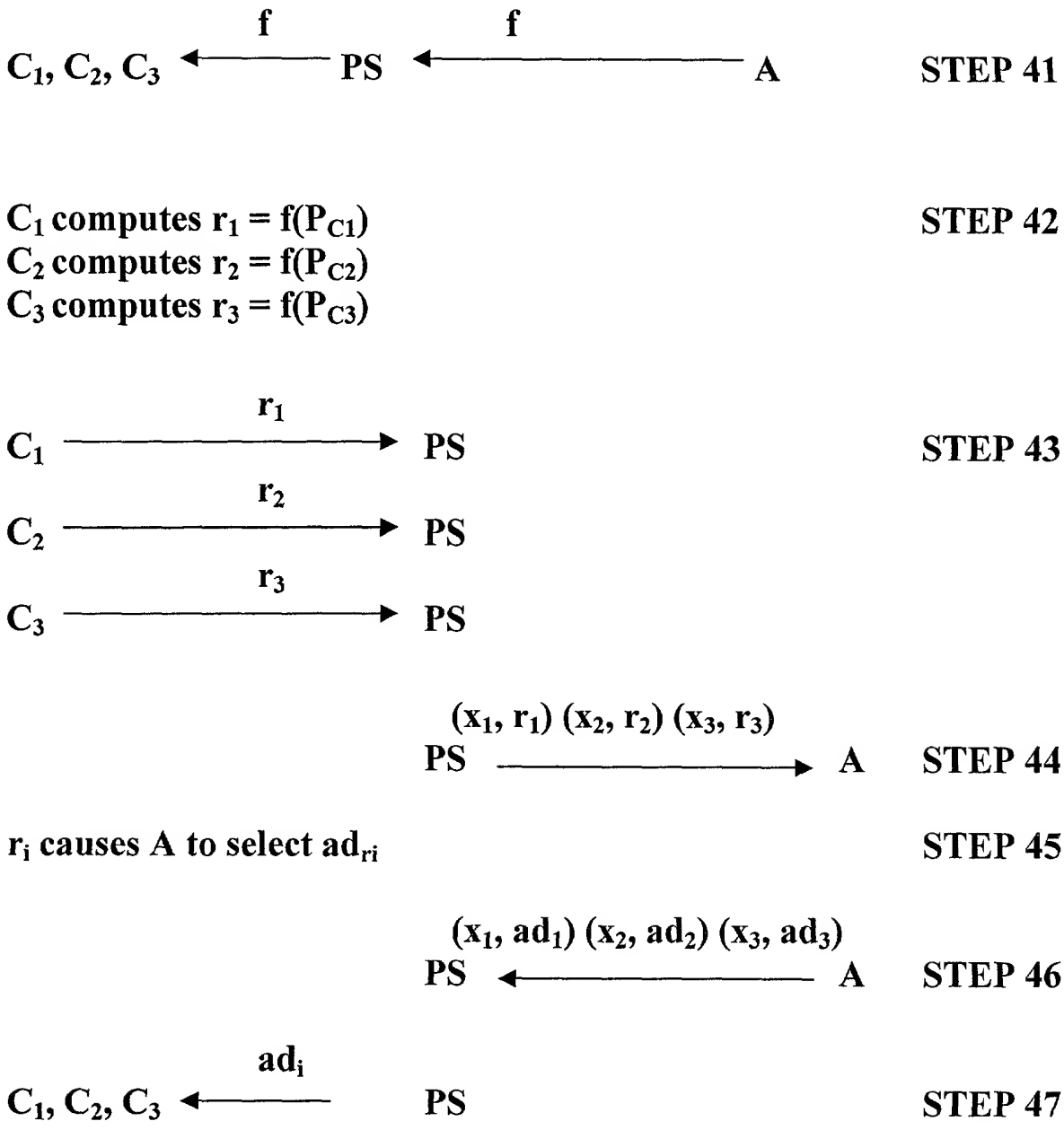
f
f
C1, C2, C3
PS
A
STEP 41
C1 computes r1 = f(PC1)
C2 computes r2 = f(PC2)
C3 computes r3 = f(PC3)
STEP 42
r1
C1
PS
STEP 43
r2
C2
PS
r3
C3
PS
(x1, r1) (x2, r2) (x3, r3)
PS
A
STEP 44
ri causes A to select adri
STEP 45
(x1, ad1) (x2, ad2) (x3, ad3)
PS
A
STEP 46
adi
C1, C2, C3
PS
STEP 47

FIGURE 4

STEP 51 $C_1, C_2, C_3 \xleftarrow{f}$ **A**

STEP 52 **C_1 computes $r_1 = f(P_{C1})$ and encrypts $E_y[r_1]$**
C_2 computes $r_2 = f(P_{C2})$ and encrypts $E_y[r_2]$
C_3 computes $r_3 = f(P_{C3})$ and encrypts $E_y[r_3]$

STEP 53 $C_1 \xrightarrow{\{E_y[r_1], x_1\}}$ **BB**
$C_2 \xrightarrow{\{E_y[r_2], x_2\}}$ **BB**
$C_3 \xrightarrow{\{E_y[r_3], x_3\}}$ **BB**

STEP 54 Servers collect $V_1 = \{E_y[r_i], x_i\}_{i=1}^{k}$

STEP 55 Servers mix V_1 by random secret permutation σ_1
to obtain $V_2 = \{r_{\sigma 1(i)}, E_y[\sigma_1(i)]\}_{i=1}^{k}$

STEP 56 Servers replace each r_j in V_2 with ad_{rj}
to obtain $V'_2 = \{ad_r, E_y[\sigma_1(i)]\}_{i=1}^{k}$

STEP 57 Servers mix V'_2 by random secret permutation σ_2
to obtain $V_3 = \{(E_y[ad_{\sigma 2(i)}], \sigma_2(i)\}_{i=1}^{k}$

STEP 58 Servers apply quorum controlled asymmetric proxy re-encryption
to obtain $V_4 = (E_{yci}[ad_{ri}], i)_{i=1}^{k}$.

STEP 59 $C_1, C_2, C_3 \xleftarrow{E_{yci}[ad_{ri}]}$ **A**

STEP 60 C_1, C_2, C_3 decrypt $E_{yci}[ad_{ri}]$ to receive ad_{ri}

FIGURE 5

STEP 61 C $\xleftarrow{\mathbf{f}}$ A

STEP 62 **C computes r = f(P) and encrypts $E_y[r]$**

STEP 63 C $\xrightarrow{E_y[r_1]}$ **BB**

STEP 64 Servers encrypt ad_i to generate $U_1 = \{(j, E_y[ad_j])\}^n_{j=1}$

STEP 65 Servers mix U_1 by random secret permutation σ to obtain $U_2 = (E_y[\sigma(j)], E_y[ad_{\sigma(j)}])^n_{j=1}$

STEP 66 Servers perform a distributed plaintext equality test to find $E_y[j] \sim E_y[r]$ and obtain $U_3 = (E_y[r], E_y[ad_r])$

STEP 67 Servers apply quorum controlled asymmetric proxy re-encryption to obtain $E_{yci}[ad_r]$

STEP 68 C $\xleftarrow{E_{yci}[ad_r]}$ A

STEP 69 C decrypts $E_{yci}[ad_r]$ to receive ad_r

FIGURE 6